Atos Microsoft Sentinel as a Service

Having invested in Microsoft O365 and Microsoft Azure for the business benefits, how will your cloud assets be secured and who is monitoring, detecting, and responding to security incidents?

Customers adopt Microsoft Azure Cloud to achieve business goals and rarely for security purposes. However, when moving to Azure Cloud, a business puts resources, assets, workflows, and data in the cloud that are crucial to business survival and consequently need strong protection against cybersecurity risks.

Even if security controls and policies are correctly setup for the original migration to O365 and Azure, Microsoft is releasing new security features to keep you safe from continuously evolving cyber threats that pose a risk to your business assets and operations. There is a continuous demand to keep the security controls and policies tuned, make the best of new security features in your Microsoft/Azure subscriptions, and keep a watchful eye on security alerts.

Our Microsoft Sentinel from Atos offering uses Microsoft Sentinel to monitor your IT estate and use the Microsoft native security controls to protect and secure your business. We help you extract the most benefit from your Azure subscriptions and make sure your protection evolves with Microsoft's security advancements.

Business challenge of mitigating security risk

Customers typically adopt Azure to achieve business goals such as capex reduction, business agility or accelerating business transformation. However, the move to Azure must prompt a reassessment of the security requirements involved in protecting a business against cybersecurity risks.

This presents the business with many challenges:

1 finding skilled Azure security resources 24x7 to use Azure native security controls effectively

2 keeping pace with Azure capabilities and changes in the platform's vulnerabilities and risks

3 getting security visibility across all Azure assets

4 responding rapidly enough to cloud security incidents when they grow and multiply at 'the speed of cloud'

5 protecting a dynamic estate that varies in terms of scale and Azure subscriptions

6 getting the original business benefit of Azure without exposing the business to unacceptable cybersecurity risks

7 keeping security off the critical path for user experience, agility, and continuous integration/ deployment goals

8 building a security roadmap that protects and supports the business strategy without hindering it

9 resourcing a security solution that makes best use of valuable in-house security personnel.

Atos

Resources

We are recognized by Gartner as the number 1 worldwide in managed security services by revenue. We have over 6,500 security experts, 16 Security Operation Centers and process 31 billion security events per day.

Atos is also positioned as a Leader in Gartner's Magic Quadrant for Data Center Outsourcing and Hybrid Infrastructure Managed Services for both Europe and North America.

Atos Managed Microsoft Sentinel – Enterprise benefits

The service benefits for the customer enterprise are:

- Optimized utilization of native Azure security controls to achieve compliance and risk mitigation
- Standardized Azure resource security by driving 'security by policy' to ensure that the appropriate security controls are in place whenever new Azure resources are created
- Relief from alert fatigue on the in-house security team by using Atos security automation to reduce workload
- Avoiding Azure cross-training of in-house security staff
- Accessing skilled, cost effective 24x7 Security Operations Centers
- Reducing incident tickets through Atos SOC triage and use of automated responses
- 'Shift-Left' of security in the DevOps lifecycle by setting security policy and monitoring compliance from start of DevOps lifecycle

- Faster incident response by automated remediation responses
- Improved incident response consistency and effectiveness by playbooks and automation
- Flexible SOC staffing worldwide
- Leveraging Atos investment in security playbooks
- Service improvements from the Atos experience with other customers and other industries
- Customization to the customer's specific security risks and needs via additions to the core service
- Predictable, planned journey to achieve the security maturity appropriate to the customer's business risks and budget.

Securing your business

Service onboarding occurs in 2 phases – Core and Customized. The Core Service quickly implements security visibility across your Azure estate within 30 days or less. This secures your Azure assets using your existing subscriptions and the default Azure security controls and recommendations, maximizing the value of the Azure security features you have already bought in your subscriptions. As a member of the Microsoft Intelligent Security Association (MISA) and the Cybersecurity Tech Accord, Atos is well positioned to utilize Microsoft and partner technology to defend your business in a world of increasing threats.

Once the Core Service is complete and when you are ready, we offer the Customized Service to collaborate with you to create business risk driven security controls specific to your business. This service builds a security roadmap that matches your specific business goals, vulnerabilities, threats, and adversaries.

If additional, non-security Azure skills are needed, then Atos, who has been a Microsoft Strategic Alliance Partner for over 20 years, can call upon the global Atos Microsoft practice of over 3,300 cloud experts to address your additional business challenges.

Next steps

It's important that our service secures your business assets and operations using the native security controls and features that are built into Microsoft and Azure. We will work with you to identify your key assets, operations and services to design a security service that matches your risk appetite and mitigates the threats you face. Our Security Architects start by making effective use of the security features in your existing Microsoft and Azure subscriptions. Our 24/7 Security Operations Center

(SOC) quickly establishes security visibility with round the clock monitoring of your security alerts and security policy breaches. With the basics covered we will tune and develop the service at your pace to meet your specific security needs.

Atos has the skills, methods, resources, and partner relationships that you need to secure your business whether you are a specialist enterprise or a large multinational.
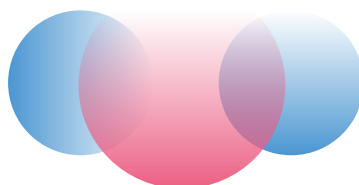
Why secure your Azure assets and services with Atos?

Atos is ranked the number 1 in Managed Security Services (MSS) in terms of 2021 MSS revenue, according to the 2022 Gartner report, operating sixteen 24/7 Security Operations Centers worldwide, providing cybersecurity services to national and global clients across all sectors. Atos is a trusted partner and digital services leader delivering end-to-end security advice, support and solutions. This means:

- **Relevant security, tailored to your security risk**. Given the wealth of technical material on the cyber threat, threat actors and their motivations, understanding what this really means for your organization can be a challenge. Atos can work with your senior team to diagnose the threat you face and the associated business risk, advise on investment choices and embody a culture of cyber maturity into your people and ways of working.

- **Resilient services based on evergreen technology.** We design, build and run security as a service to keep up with the latest technologies so you don't have to. This delivers enterprise-grade security leveraging existing investments in Azure cloud subscriptions and assets to deliver value for money in detection, protection and service.

- **Improved confidence.** A partnership with Atos means effective support in good times and bad. You will have visibility of what really is happening in your Azure cloud, insight into how this affects your sensitive data and practical help in the event of compromise.

Atos and Microsoft

The Atos - Microsoft Strategic Alliance has existed for over 20 years with:

- global Microsoft practice with +3,300 Cloud experts
- +1,700 dedicated Microsoft Consulting Specialists
- +850 Microsoft consultants in Global Delivery Center
- Microsoft Azure Expert Managed Service Provider since July 2019.
- Atos joined Microsoft Intelligent Security Association (MISA) in 2020

Member of
Microsoft Intelligent
Security Association

Microsoft

For more information: atos.net/cloud-security/atos-and-microsoft-azure